



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado

**Propuesta de un modelo conceptual de preservación
digital aplicable a la mejora de la preservación de
evidencia digital en instituciones de investigación
criminal**

TESIS

Para optar el Grado Académico de Doctor en Ingeniería de
Sistemas e Informática

AUTOR

Fernando Tiverio MOLINA GRANJA

ASESOR

Glen Dario RODRÍGUEZ RAFAEL

Lima, Perú

2017



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Molina, F. (2017). *Propuesta de un modelo conceptual de preservación digital aplicable a la mejora de la preservación de evidencia digital en instituciones de investigación criminal*. [Tesis de doctorado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

1133



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMÉRICA
Facultad de Ingeniería de Sistemas e Informática
UNIDAD DE POSGRADO



1767
213

SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE DOCTOR EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

En la Ciudad Universitaria, a los dieciocho (18) días del mes de setiembre del 2017, siendo las 19:00 horas, se reunieron en el Auditorio de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, el Jurado Examinador de tesis conformado por los siguientes profesores:

- Dr. David Santos Mauricio Sánchez (Presidente).
- Dr. Glen Darío Rodríguez Rafael (Miembro Asesor).
- Dr. Hugo Froilán Vega Huerta (Miembro).
- Dra. Nora Bertha La Serna Palomino (Miembro).
- Dra. Luz Sussy Bayona Oré (Miembro).

Se inició la Sustentación de la tesis invitando al magister **Fernando Tiverio Molina Granja** para que realizara la exposición oral y pública de la tesis para optar el Grado Académico de Doctor en Ingeniería de Sistemas e Informática, siendo la Tesis intitulada:

“Propuesta de un Modelo Conceptual de Preservación Digital Aplicable a la Mejora de la Preservación de Evidencia Digital en Instituciones de Investigación Criminal”

Concluida la exposición, los miembros del Jurado Examinador procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

DIECIOCHO (18) - MUY BUENO

Por tanto el Presidente del Jurado, de acuerdo al Reglamento de Grados y Títulos, le otorga al magister **Fernando Tiverio Molina Granja** el Grado Académico de Doctor en Ingeniería de Sistemas e Informática.

Siendo las... 21:00 horas, el Presidente del Jurado Examinador da por concluido el acto académico de Sustentación de Tesis.

DR. DAVID SANTOS MAURICIO SÁNCHEZ
Presidente

DR. GLEN DARIÓ RODRÍGUEZ RAFAEL
Miembro Asesor

DR. HUGO FROILÁN VEGA HUERTA
Miembro

DRA. NORA BERTHA LA SERNA PALOMINO
Miembro

DRA. LUZ SUSSY BAYONA ORE
Miembro

RESUMEN

Cualquier dispositivo digital genera información que puede convertirse en evidencia valiosa para un juicio en caso de presentarse un incidente de seguridad, cibercriminal o de ataques informáticos, el problema es que muchas veces la recolección, el manejo y la preservación de esta evidencia no se realizan de manera adecuada.

Esta investigación se centra en la preservación de evidencia digital. Una vez que se ha obtenido la información y evidencia de los dispositivos digitales motivo del delito, es muy importante mantener y preservar dicha información desde que inicia el proceso legal, durante la investigación y hasta que finalice el juicio o la investigación para garantizar que no exista contaminación, daño, alteración o manipulación de la evidencia y de esta forma mantener la confiabilidad en el proceso, especialmente en el largo plazo. Así, la preservación de la evidencia digital es un aspecto de importancia al momento de decidir la admisibilidad de la evidencia digital en un proceso judicial vigente, o en un futuro proceso, reabierto por apelaciones u otro motivo, o como fuente de información histórica.

De la revisión de literatura se determina un conjunto de aspectos mínimos necesarios que aplicados efectivamente al Modelo OAIS¹ (Consultative Committee for Space Data Systems, 2012), genera un marco de referencia para aumentar la admisibilidad de la evidencia digital en el largo plazo en instituciones de investigación criminal, en este mismo ámbito, los modelos más utilizados PREMIS², OAIS, DAMM³, NDSA⁴, requieren de características adicionales para cubrir las necesidades de preservación de evidencia requeridos por las autoridades judiciales.

Así, de la investigación se desprende los aspectos relevantes que expresamente no poseen los modelos mencionados, y que para el ámbito de las instituciones de investigación criminal son determinantes y fundamentales, estos son: Museo de Herramientas, Terminología, Control de calidad ingesta, Ingesta parcial, Metadatos del entorno de la evidencia a preservar, Garantizar la integridad del original, Evaluación de riesgos, Almacenamiento distribuido, Tiempo de preservación, Certificaciones de la estrategia.

De la misma manera, se define como requisitos mínimos de admisibilidad, los siguientes: La legalidad de la evidencia, El respeto por los derechos fundamentales, La fiabilidad de las

¹ Open Archival Information System

² Data Dictionary for Preservation Metadata

³ The Digital Accessibility Maturity Model

⁴ National Digital Stewardship Alliance

evidencias, junto con su pertinencia, La efectividad de los mismos, El respeto a las normas de protección de datos, El respeto del secreto de las comunicaciones y respeto por el derecho a la libertad de expresión, Confidencialidad, Autenticidad, Integridad, Roles de responsabilidad de ingesta y de administración, Creación de evidencia Digital, Transmisión de evidencia Digital, Almacenamiento de información, entre otros; documentación que debe ser creada y mantenida para registrar de ser posible, cada paso del ciclo de vida preservación de la evidencia, adicional se indica que se elimina del modelo OAIS toda opción de actualización de contenidos ya ingresados, pues por definición la evidencia digital debe permanecer intacta.

El modelo es validado por expertos, es así que, se tomaron datos del personal involucrado en el sistema de justicia de la Ciudad de Riobamba, que en adelante se lo tratará como “Actores”, y que actúan en la preservación de la evidencia digital y en la decisión de admitir la evidencia en un juicio, así, con la totalidad de la población que es de 74 actores, distribuidos en 5 Custodios de Evidencia, 24 Fiscales, 35 Jueces, 5 Peritos Informáticos, y 5 Técnicos Administradores del modelo, los actores realizaron un cuestionario (ver anexo 2), validado con un Alfa de Conbranch de 0,83, previamente diseñado, basado en NESTOR (Nestor working Group, 2009), que evalúa la importancia de dimensiones como la Infraestructura organizacional, la Administración de objetos digitales, la Gestión de la infraestructura y riesgos de seguridad, y la Gestión de aspectos de integridad en instituciones de investigación criminal.

Como resultado del análisis estadístico global de los actores, se determina que las cuatro dimensiones influyen altamente en la determinación del nivel de admisibilidad de la evidencia digital en la corte, por lo que la aplicación de un modelo de preservación de evidencia digital para instituciones de investigación criminal denominado PREDECI (Molina & Rodriguez, 2017b), garantiza una mayor admisibilidad de la evidencia en la corte.

Adicionalmente se desarrolla un aplicativo prototipo para evidenciar la funcionalidad y usabilidad del modelo, y es evaluado en las mismas condiciones (Cuestionario y entorno) por los actores en cinco casos específicos, obteniendo en general una aceptación adecuada del aplicativo como herramienta para preservar la evidencia digital en términos de elevar la admisibilidad. Esto permite determinar que es un prototipo que puede aplicarse para procedimientos de preservación de evidencia digital.

Finalmente, esta investigación ha generado hasta el momento 7 publicaciones en forma de artículos científicos, en seminarios, congresos y revistas con factor de impacto mundial, lo que apoya la importancia e impacto de la presente investigación.

Palabras Clave: Preservación Digital, Evidencia Digital, Repositorios Digitales, PREMIS, PREDECI, OAIS, DAMM, NDSA, Admisibilidad, Investigación Criminal, Preservación de Evidencia Digital.

ABSTRACT

Any digital device generates information that can become valuable evidence for a trial in the event of a security incident, cybercriminal or computer attacks, the problem is that the collection, handling, and preservation of this evidence is often not performed in an appropriate manner.

This research focuses on the preservation of digital evidence. Once the information and evidence of digital devices has been obtained, it is very important to maintain and preserve such information from the beginning of the legal process, during the investigation and until the end of the trial or investigation to ensure that there is no contamination, Alteration or manipulation of evidence and thus maintain reliability in the process, even in the long term.

The preservation of digital evidence is an important aspect when deciding admissibility in a judicial process in force, or in a future process, reopened by appeals or other reasons, or as a source of historical information.

From the literature review, a set of necessary minimum aspects that are effectively applied to the OAIS Model is determined, generating a frame of reference to increase the admissibility of digital evidence in the long term in research institutions, in this same area, the most Used PREMIS, OAIS, DAMM, NDSA and analyzed in this research, require additional features to cover the needs for preservation of evidence required by judicial authorities.

Thus, the investigation reveals which are the relevant aspects that expressly do not have the mentioned models and that for the scope of criminal investigation institutions are determinant and fundamental, these are: Museum of Tools, Terminology, Quality control ingestion, Partial ingestion, Metadata of the environment of the evidence to be preserved., Guarantee the integrity of the original, Risk assessment, Distributed Storage, Preservation time, Certifications of strategy.

The following are defined as minimum admissibility requirements: The legality of the evidence, respect for fundamental rights, The reliability of the evidence, together with its relevance, the effectiveness thereof, respect for the rules of protection of Confidentiality, Integrity, Responsibility of ingestion and administration of responsibility, creation of Digital evidence, Transmission of Digital Evidence, Storage of information, data protection, respect for the secrecy of communications and respect for the right to freedom of expression, among

others; Documentation that must be created and maintained to record if possible each step of the life cycle preservation of evidence. PREDECI eliminates from the OAIS model any option of updating already entered contents because by definition the digital evidence or should not remain intact.

Based on the OAIS preservation model, metadata concepts and the relevant requirements and aspects mentioned, necessary for digital preservation in criminal investigation institutions, this research proposes as input a reference model for the Preservation of Digital Evidence, known as PREDECI , Applicable in criminal investigation institutions that have the responsibility to guard it over the long term in order to increase the admissibility of digital evidence in the court or the availability of evidence to a community designated to handle evidence, ensuring fidelity and Integrity of the company over the long term. It responds to a set of responsibilities determined in laws and regulations for this environment.

A validation by experts is applied, so data were taken from the personnel involved in the justice system of the City of Riobamba, who will henceforth be treated as "Actors", and who act in the preservation of digital evidence and In the decision to admit the evidence in a trial, thus, with the totality of the population that is 74 actors, distributed in 5 Custodians of Evidence, 24 Prosecutors, 35 Judges, 5 Computer Experts, and 5 Technical Administrators of the model, the Actors carried out a questionnaire (see Annex 2), validated with a previously designed 0.83 conbranch alpha, based on NESTOR (Nestor working Group, 2009), which evaluates the importance of dimensions such as Organizational Infrastructure, Object Management Digital management, infrastructure management and security risks, and the management of integrity aspects in criminal investigation institutions.

As a result of the global statistical analysis of the actors, it is determined that the four dimensions influence highly the determination of the level of admissibility of digital evidence in the court, so the application of a PREDECI digital evidence preservation model guarantees a Greater admissibility of evidence in the court.

Additionally, a prototype application is developed to demonstrate the functionality and usability of the model and is evaluated in the same conditions (Questionnaire and environment) by the actors of five specific cases, obtaining, in general, an adequate acceptance of the application as a tool to preserve the digital evidence In terms of raising eligibility. This allows determining that it is a prototype that can be applied for digital evidence preservation procedures.

Finally, this research has generated 7 publications in the form of scientific articles, seminars, congresses, and journals with a global impact factor, which supports the importance and impact of the present research.

Keywords: Digital preservation, Digital Evidence, Digital Repository, PREMIS, PREDECI, OAIS, DAMM, NDSA, Admissibility, Criminal Investigation, Preservation of Digital Evidence.